North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

$4.5 million repair recommended for Jamestown sewer system. Concluding its study of Jamestown's sanitary sewer system, Ulteig Engineering recommends a $4.5 million fix that will hopefully get the city safely through another flood event. The Ulteig engineer in charge of the study took the City Council's Public Works Committee through details of the system's flows and inadequacies the week of November 23. This was the second update on the study, dealing with a deficiency evaluation, lift station and pipe capacities, and priorities for handling wastewater throughout the system. He said the city's system is not all that different from other communities. The biggest problem in Jamestown is the adverse effect of the James River and Pipestem Creek on the sewer system. Of the three alternatives presented, Ulteig's preferred option offers some ways to mitigate that effect.The alternative calls for running the wastewater from lift station No. 8 near the Second Street Southwest bridge to lift station No. 9 in the Jamestown Business Center parking lot. From there construction of a new force main to lift station No. 1 in the area of Business Loop East would direct the wastewater away areas of high infiltration. Source: http://www.grandforksherald.com/event/article/id/184667/group/homepage/

Second 'frac' spill worries officials. Two spills during oil well fracture treatments in four months — the last one November 20 — has North Dakota's chief oil regulator poised to bear down to prevent more incidents as drilling intensifies in the oil patch. The head of the state's Department of Mineral Resources, said he plans an in-house review of drilling policies to make sure they are adequate to prevent future repeats. His agency was already preparing for a complaint against Denbury Resources of Texas, for an apparent violation that caused a fracture blowout and 2,500-gallon spill near Killdeer in early September. November 20's spill occurred at a Whiting Petroleum Corporation well eight miles northwest of New Town. The well was shut down after 5,600 gallons of chemical-laced fracture water and 420 gallons of oil were spilled inside a lined dike around the well. Since 2008, after four wells failed during fracture treatments, North Dakota has required that drillers install pressure relief valves to prevent blowouts. The Killdeer well blew out when the fracture pressure spiked up to 9,000 psi, a third higher than normal, without adequate relief valving. That spill also was contained within a dike. Groundwater monitoring around the Killdeer well detects no contamination. Source: http://www.bismarcktribune.com/news/local/article_ad40e1b8-f78f-11df-be35-001cc4c002e0.html

North Dakota oil well shut down after spill. A Denver-based energy company has shut down an oil well in northwestern North Dakota after a spill. Whiting Petroleum Corp. said a valve failure led to the spill November 20 about 8 miles northwest of New Town. Workers at the site were evacuated, but Whiting said the spill was in a rural area and no residents had to be evacuated. No injuries were reported. The company said oil, water, and natural gas spilled. There was no immediate estimate on spill amounts. Source: http://www.grandforksherald.com/event/article/id/184328/group/homepage/

Another flood survery from the Corps. The Army Corps of Engineers said it is working on a new plan that would eliminate any impacts on people living downstream from a Fargo-Moorhead diversion in

North Dakota and Minnesota. The plan would involve two major changes: The first would include a large water storage area just north of the diversion inlet. That would put it roughly south and east of Horace, North Dakota. The second would involve a levy and gates that would back up the Red River to the south of the diversion by 3 to 7 feet. The biggest result would be no additional downstream flooding. A Corps spokesman said impacts would be felt to the south of the diversion for up to 7 miles. That is better than the hundreds of miles expected to be impacted north of the Fargo-Moorhead area under the other plans. A Cass County commissioner said 800 homes could be affected to the south, including the Oxbow, Minnesota area. That compares to more than 4,000 homes that would be affected to the north of Fargo-Moorhead. Source: http://www.kfgo.com/news_Detail.php?ID=11971

REGIONAL

(Minnesota) **MDA confirms first detection of brown marmorated stink bug in Minnesota.** Late the week of November 15, Minnesota Department of Agriculture (MDA) laboratory staff in St. Paul found a brown marmorated stink bug on some new equipment that had been delivered to the lab building. The staff contacted the MDA's Plant Protection Division, where staff confirmed the insect was the first brown marmorated stink bug found in the state. Native to Asia, the pest was first identified in the United States in Pennsylvania in 2001. It has since been reported across the mid-Atlantic region and in Oregon. The bug typically spreads to new areas by flying or by stowing away in shipping containers or vehicles. It is unclear how the insect arrived in the laboratory building. However, MDA's plant protection director said it is likely the insect hitched a ride inside the boxes containing the new lab equipment, which had been shipped from the eastern U.S. In response to this discovery, MDA is searching the laboratory to find and eradicate any other stink bugs that may have arrived. Source: http://www.reviewmessenger.com/index.php?option=com_content&view=article&id=8098:mda-confirms-first-detection-of-brown-marmorated-stink-bug-in-minnesota&catid=35:other-local-news

(Minnesota) **DEET chemical now being found in municipal water supplies.** The Minnesota Department of Health (MDOH) is conducting an investigation into the popular insect repellent N,N-Diethyl-meta-toluamide (DEET), in response to concerns over its prevalence in groundwater, rivers and lakes that serve as drinking water sources. DEET has also been detected downstream of wastewater treatment plants. "We shower, it goes down the drain, and it ends up in wastewater that goes into rivers," a state toxicologist said. DEET, the active ingredient in most chemical insect repellents, may be toxic to the nervous system. Little is known about DEET's effects if ingested in drinking water. A 2004 U.S. Geological Survey study found it was among the top 10 most commonly detected chemicals in a survey of 65 Minnesota lakes and streams. A 2006 study confirmed the chemical's presence in one-third of 43 Mississippi River sites tested in the state, while a 2009 study found it in every one of 12 lakes and four rivers tested. As a consequence, MDOH designated DEET as one of seven "chemicals of emerging concern" whose safety it will assess during the coming year. Source: http://www.naturalnews.com/030446_DEET_water_supply.html

(Montana) **Gas vapors under Miles City Post Office prompt evacuation order.** In Montana, the Miles City Post Office was evacuated after fuel vapors were detected in the offices on the building's main floor November 17. The gasoline leak was first discovered in the basement of the Lewis and Clark apartment building next to the Conoco Short Stop gas station off Seventh Street. The apartment manager reported an unusual odor to Montana Dakota Utilities October 25. The apartment building

was evacuated. Crews from the state Department of Environmental Quality (DEQ) were working to mitigate the vapors from the apartment so residents could return. It was believed about 9,700 gallons of fuel leaked from one of the tanks at the Short Stop. The DEQ brought in interior and exterior vapor extraction units that collect the gas fumes. More of the vapor extraction units were expected to arrive next week. The DEQ will continue to monitor the size of the gasoline plume and track its spread using ground wells and the water table. Postal operations and customer retail service will move to 715 Haynes Ave. beginning November 19, according to a press release from the U.S. Postal Service. The post office is expected to reopen the week after Thanksgiving. Source: http://billingsgazette.com/news/state-and-regional/montana/article_7c982106-c976-582a-8123-4ddf191e9ae7.html

National

(Colorado) **Uranium exploration to expand by 2,220 acres.** County commissioners on November 23 narrowly passed a resolution approving expanded uranium exploration in the Tallahassee Creek area of Colorado, putting into place stringent guidelines aimed at protecting water. The commission voted 2-1 to allow Australia-based Black Range Minerals' request to expand exploration on an additional 2,220 acres of property known as the Hansen Deposit, which is believed to be the largest uranium deposit in the district. In passing the resolution, commissioners also put into place 34 conditions the company must abide by to continue exploration. A Black Range explorations manager asked the commission to consider changing one of the conditions from twice-a-year water well monitoring to once a year. He also requested the proposed water sampling take place twice a year on wells within a half-mile of exploration areas and only once a year for wells outside of the half-mile range. The commission denied that request. The Commission chairman said the stringent conditions may be unprecedented for prospecting and exploration. Source: http://www.tradingmarkets.com/news/stock-alert/blkmf_uranium-exploration-to-expand-by-2-220-acres-1328834.html

(Washington) **66,000 in dark as storm bears down on Washington.** Tens of thousands of people in the Puget Sound area were in the dark as a winter storm barreled through Washington state. A Puget Sound Energy spokeswoman said of the 66,000 customers without power November 23, 56,000 were in Kitsap County. She said tree branches being blown into power lines by strong winds were to blame for the outages that peaked at 90,000. The spokeswoman said if the winds continued to be a problem through November 23, more power outages were possible. The National Weather Service has posted a winter weather advisory for most of Western Washington while Eastern Washington is bracing for a rare blizzard. Source: http://www.seattlepi.com/local/6420ap_ap_us_western_weather_power_outages.html

(Washington) **Secret Service: Seattle cyber attack larger than first thought.** Federal agents now say the recent Seattle, Washington, cyber attack was a much bigger crime than first thought. A U.S. Secret Service spokesman said more than 1,000 accounts may have been compromised. "We are very close to pinpointing the actual person or persons who perpetrated this crime," he said. The scheme appears to involve the sale or distribution of the stolen account information to numerous individuals across the country, as well as foreign countries. Those individuals then used the information to make purchases against the consumer accounts. The spokesman said the trail leads overseas, with the data stolen October 22 via a one-day computer hack. At this time, evidence points to only one hacker. And

now only one business appears to have been hacked. The popular Broadway Grill said it started working with police as soon as the fraud was uncovered last month, and immediately reinforced it's computer security. Source: http://www.komonews.com/news/consumer/108568029.html

International

Norwegian airport terminal evacuated over suspicious item. A terminal at Bergen airport in Oslo, Norway was evacuated November 23 over a suspicious piece of luggage. Baggage handlers spotted an item which resulted in the decision to evacuate the terminal building, police told local media. Bomb disposal experts were heading to Bergen from Oslo, police added. Police were also trying to trace the owner of the luggage that had been checked in. The terminal was expected to remain closed for several hours. Source: http://www.monstersandcritics.com/news/europe/news/article_1600886.php/Norwegian-airport-terminal-evacuated-over-suspicious-item

11 alleged gang members killed by Mexican troops. A gun battle between Mexican soldiers and drug cartel gunmen near the border of Texas killed 11 alleged gang members and prompted the U.S. to reinforce security at international crossings, officials said November 18. The soldiers came under fire November 17 when they were investigating a tip about the presence of armed men in the town of Nueva Ciudad Guerrero in Tamaulipas, the Mexican Defense Department said in a statement. Eleven of the gunmen were killed in the ensuing gun battle but no troops were hurt, it said. Afterward, soldiers arrested two surviving gunmen who told authorities they belonged to the Zetas drug gang, the statement said. Troops also seized nine assault rifles, four handguns, a grenade launcher, and ammunition. Source: http://topnews360.tmcnet.com/topics/associated-press/articles/2010/11/22/119569-11-alleged-gang-members-killed-mexican-troops.htm

Namibian officer charged with smuggling explosive. A Namibian court has charged a senior airport police officer with placing a fake bomb at an airport in the country's capital last week. The court said November 22 that a chief inspector of the Namibian police aviation security faces charges for smuggling a suspected explosive device, using the device in an airport, and giving false information that interfered with airport operations. The suspicious device, found on a conveyor belt with luggage on a Germany-bound flight, did not contain explosives, but airport security did not know that when it was discovered November 17 at the Windhoek airport. Germany is on alert because of warnings of heightened terrorism threats. Source: http://www.foxnews.com/world/2010/11/22/namibian-officer-charged-smuggling-explosive/

Banking and Finance Industry

ATM outage stirs debate. Several financial institutions saw their ATM and online banking channels taken offline over the weekend of the daylight saving time change. The institutions allegedly affected by the outage, including Bank of America, Chase, U.S. Bank, Wells Fargo, Compass, USAA, Suntrust, Chase, Fairwinds Credit Union, American Express, BB&T on the East Coast, and PNC, reportedly blamed the downtime on a computer glitch related to the time-zone change. But a senior analyst at Aite Group LLC who covers banking and payments fraud, says more is likely going on behind the scenes. In fact, she says the outage could have been related to anything from a widespread malware attack to outdated technical infrastructures. —Infrastructure is certainly a problem with banks, the

analyst says. —They acknowledge it. And given the proprietary nature of most banking institutions' code, she says it is unlikely that a bug related to the time-zone would simultaneously hit all of these institutions, or at least within the same relative timeframe. —That just doesn't seem like a plausible reason for me, she says. —I think malware if probably the most likely culprit, or some sort of coordinated attack. Source: http://www.bankinfosecurity.com/articles.php?art_id=3127

(Florida) **Capital Circle NE remains closed after bomb threat.** Capital Circle Northeast in Tallahassee, Florida, remained closed in both directions between Raymond Diehl and Lonnbladh roads on November 24 as police officers and bomb squad technicians investigate a bomb threat made by a bank robber. A 56-year-old man entered Premier Bank, 3110 Capital Circle NE, said that he had a bomb and demanded money from a teller, said a spokesman for Tallahassee Police Department (TPD). There were customers in the bank at the time of the robbery, but no injuries have been reported. Capital Circle should be reopened within an hour, the spokesman said. Police officers arrived before the man could exit the bank, and he was taken into custody without incident. The man then claimed the bomb threat was merely a bluff, but law-enforcement officials are required to take the threat seriously. The Big Bend Regional Bomb Squad, comprised of officials from TPD, the Tallahassee Fire Department, Florida Capital Police, and other local law-enforcement agencies, deployed a robot to the bank earlier in the morning. Investigators also examined a secondary search site, the parking lot of Gold's Gym, 2695 Capital Circle NE, where they think the man may have parked his car. Source: http://www.tallahassee.com/article/20101124/BREAKINGNEWS/101124004/Updated--Capital-Circle-NE-remains-closed-after-bomb-threat

Crooks rock audio-based ATM skimmers. Criminals increasingly are cannibalizing parts from handheld audio players and cheap spy cams to make extremely stealthy and effective ATM skimmers, devices designed to be attached to cash machines and siphon card + PIN data, a new report warns. The European ATM Security Team (EAST) found that 11 of the 16 European nations covered in the report experienced increases in skimming attacks last year. EAST noted that in at least one country, anti-skimming devices have been stolen and converted into skimmers, complete with micro cameras used to steal PINs. EAST said it also discovered that a new type of analog skimming device — using audio technology — has been reported by five countries, two of them "major ATM deployers" (defined as having more than 40,000 ATMs). Source: http://krebsonsecurity.com/2010/11/crooks-rock-audio-based-atm-skimmers/

FBI raids three hedge funds in insider trading case. The FBI raided three hedge funds as part of a widening probe into suspected insider trading in the $1.7 trillion hedge fund industry. The November 22 raids come as federal prosecutors prepare to unveil a series of new insider trading cases as soon as this year against hedge fund traders, consultants and Wall Street bankers. Two of the raided funds are Diamondback Capital Management LLC and Level Global Investors LP, each based in Connecticut and run by former managers of SAC Capital Advisors, one of the best-known U.S. hedge funds. A Boston, Massachusetts-based firm, Loch Capital Management, was also raided, a person familiar with the matter said. Loch has close ties with a witness who pleaded guilty in an insider trading probe centered on hedge fund Galleon Group. —The Justice Department promised a more muscular approach to white-collar crime, and is delivering, said a professor at the City University of New York's John Jay College of Criminal Justice. Spokesmen for the FBI in New York and Boston said

November 22 that the agency had executed search warrants in connection with an ongoing investigation. Source: http://www.reuters.com/article/idUSLNE6AM01N20101123

Feds probing mutual funds in alleged insider trading ring: Report. Federal authorities are examining whether multiple insider-trading rings reaped illegal profits totaling tens of millions of dollars, the Wall Street Journal reported November 20, citing people familiar with the matter. The 3-year criminal and civil investigation could result in charges by the end of the year, the Journal reported. A federal grand jury in New York has heard evidence, the paper said. One focus of the investigation is whether independent analysts and consultants who work for companies that provide "expert network" services to hedge funds and mutual funds passed along nonpublic information, the Journal reported. Such companies set up meetings and calls between current and former managers and traders who want an investing edge. The newspaper said one firm under examination is Primary Global Research LLC of Mountain View, California, which connects experts with investors seeking information in the technology, health care, and other industries. The firm's Web site said the chief operating officer and the firm's CEO previously worked for Intel Corp. Prosecutors and regulators are also examining whether bankers from Goldman Sachs Group Inc. leaked information about transactions, including health-care mergers, to the benefit of certain investors, the Journal reported. Source: http://www.investmentnews.com/article/20101122/FREE/101129995

Cleveland Federal Reserve hacked. A 32-year-old Malaysian man was arrested shortly after his arrival last month at John F. Kennedy International Airport in New York City. Authorities said he hacked into the Cleveland Federal Reserve Bank and several other computer systems, including a defense contractor. The Malaysian national faces a four-count indictment that charges him with hacking into computer systems, and the possession of more than 400,000 stolen credit and debit card numbers. "Cybercriminals continue to use their sophistication and skill as hackers to attack our financial and national security sectors," said the United States Attorney for the Eastern District of New York. The suspect's arrest comes just 1 month after authorities arrested a big cyber crime gang in the United States and Europe for similar crimes. When the suspect arrived in New York October 21, he was arrested hours later by Secret Service agents. The suspect, who is being held in pre-trial detention, "made a career of compromising computer servers belonging to financial institutions, defense contractors and major corporations, among others, and selling or trading the information," said the United States Attorney for the Eastern District of New York. Source: http://www.bankinfosecurity.com/articles.php?art_id=3115

Chemical and Hazardous Materials Sector

National Hazmat Fusion Center offers information-sharing Web portal. National Hazardous Materials Fusion Center officials unveiled a responder-driven data collection, analysis and education Web portal as part of a collaborative effort between the U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) and the International Association of Fire Chiefs (IAFC). The portal is the central element of the Hazmat Fusion Center, a free, voluntary, confidential, and secure Web-based portal that serves as a data and information network for hazmat teams; first responders; federal, state and local agencies; and the private sector. The Internet-based portal serves as a one-stop shop for hazmat-response information, including training packages, reports, incident-based case studies, statistics, trends, alerts, recommendations, and peer-to-peer networking. It was designed with a consistent method of information collection to support

information-sharing across jurisdictions and levels of government and to support individual and national-level needs. The secure incident-reporting system is available for hazmat teams to enter, manage and analyze their own incident reports while letting the Hazmat Fusion Center create a national picture of hazmat response and disseminate regional and national hazmat trends and statistics. There is a public and a members-only private side to the Web portal. Source: http://urgentcomm.com/networks_and_systems/news/hazmat-fusion-center-20101118/

(Nevada) **GOP seeks to revive Yucca project.** Three Republican Congressmen have served notice in a letter to the Office of Management and Budget that the battle over Yucca Mountain is far from over. The letters were written by Representatives from the states of Idaho, Washington, and Wisconsin, and they requested a review of the decision by the Nuclear Regulatory Commission (NRC) Chairman to shut down the review of the Department of Energy's (DoE) application to license the nuclear waste dump 100 miles north of Las Vegas, Nevada. They argue the issue is being litigated in federal court and that the Atomic Safety and Licensing Board rejected the DoE's motion to withdraw the license application. "I am greatly concerned by the NRC chairman's decision to unilaterally shut down the Yucca Mountain license application over the concern of other commissioners and Congress," the Idaho Representative said in the letter. The Nuclear Projects office director said the letter is nothing new. "The reason is simple: none of the other 49 states want nuclear waste in their state," he said. Source: http://www.nevadaappeal.com/article/20101119/NEWS/101119599/1070&ParentProfile=1058

Commercial Facilities

(New Jersey) **Police investigate Kinnelon mall bomb scare after woman finds threat near ATM.** Police are investigating a bomb scare at the Meadtown Mall in Kinnelon, New Jersey, after a bank customer found a threatening note near an ATM machine November 25, police said. A police officer was on patrol at 10:23 a.m. when a woman flagged him down in the mall parking lot, saying she —had to show him something, the lieutenant said. Inside the PNC Bank on a counter across from the cash machine was a handwritten note that read, —There's a bomb in the bank, he said. The Morris County Sheriff Department's bomb squad and criminal investigations division were called in but no explosives were found. No one was evacuated because most of the mall stores were closed, he said. The parking lot was secured and authorities are now searching surrounding areas. He said there have been no recent bomb threats in the area. Source: http://www.northjersey.com/news/crime_courts/112510_Police_investigate_Kinnelon_mall_bomb_scare_after_woman_finds_threat_near_ATM.html

(Delaware) **Man charged in pharmacy bomb threat, hotel robbery.** Delaware State Police have charged a Lewes man accused of making a bomb threat against a Rehoboth pharmacy and robbing a Dover hotel. Police arrested the 26-year-old man on November 24 in connection with the threat called in to the Rite Aid Pharmacy at Rehoboth Mall on October 30. Police say the man was developed as a suspect in the bomb threat during the investigation of the robbery of the Best Western hotel in Dover on October 21. He is charged with robbery, conspiracy, theft, attempted robbery, and two counts of terroristic threatening. He is being held at the Sussex Correctional Institution on $63,000 secured bail. Source: http://www.bostonherald.com/news/national/northeast/view/20101125man_charged_in_pharmacy_bomb_threat_hotel_robbery/srvc=home&position=recent

(New Jersey) **Motels evacuated, hospital searched after bomb threats in Somers Point.** Multiple bomb threats in locations throughout Somers Point, New Jersey, November 20 led to the evacuation of three motels, and a precautionary sweep of Shore Memorial Hospital. The threat came in at 11:21 a.m., a police captain said. A 911 caller told a dispatcher that "there would be three explosions at three different (specific) locations within Somers Point," as the captain described the call. "We'd only have time to save two locations and one would fall." The Somers Point emergency management coordinator said the Sunrise Motel on Bay Avenue, the Residence Inn on MacArthur Boulevard, and Pier 4 were evacuated following the threat. Shore Memorial was not specifically mentioned, he said, but the streets on either side of the main hospital building were blocked off and no one was allowed inside. Bomb-sniffing dogs from Hamilton Township and Pleasantville K-9 units swept the main building and declared it clear at about 1:15 p.m. All locations were declared clear by 1:30 p.m. Source: http://www.pressofatlanticcity.com/news/breaking/article_640d756a-f4ce-11df-86be-001cc4c002e0.html

(New York) **NY police: False report led to mall evacuation.** Police said a homeless man made a false claim about a suitcase that led to a Westchester County, New York, mall being evacuated for almost 2 hours November 20. Authorities said the man told police that a suitcase he left in the food court at The Galleria mall had been given to him by a Middle Eastern man and was ticking. The story led to the mall's evacuation around 12:15 p.m. The suitcase was examined and found to contain clothes, and the mall was reopened around 2 p.m. The man faces a charge of falsely reporting an incident. Source: http://online.wsj.com/article/AP645613751b294df7ab0a35def29710f2.html

(Colorado) **Activist admits setting fire to Colorado sheepskin store.** A self-described animal-rights activist known on the Internet as "Lone Wolf" pleaded guilty in federal court November 18 to arson in a fire that destroyed a Denver, Colorado sheepskin business. The man admitted in U.S. district court to setting the fire that burned the Sheepskin Factory to the ground April 30, 2010. The store sold sheepskin blankets, rugs, and related products. Authorities were led to the suspect after an informant told them the man — who called himself "Lone Wolf" on the Internet and has the word "Vegan" tattooed in his neck in large letters — bragged on an animal rights Web site that he "torched" the business. The man faces up to 30 years in federal prison and a maximum $500,000 fine when he is sentenced at a later hearing. The man has a prior arson conviction in Iowa and is a suspect, while not charged, in two other arson cases of a leather store and a restaurant in Salt Lake City, Utah. Source: http://wsau.com/news/articles/2010/nov/18/activist-admits-setting-fire-to-colorado-sheepskin/

Communications Sector

(Arizona) **Suspect arrested on charges of wire theft.** Prescott police recently arrested a man on charges including burglary after he sold copper wire to Yavapai Metal Recycling that he allegedly stole from Qwest. Officers booked the man into the Yavapai County Jail in Camp Verde on charges of burglary and trafficking in stolen property. On October 28, Qwest told police that he misrepresented himself by telling the company that he was subcontracting a work project with Qwest. He allegedly stole about 400 pounds of copper wire from Qwest's yard at 1445 Masonry Way, Prescott, said a spokesman for the Prescott Police Department. Shortly after the suspect left with the wire, Yavapai Metal Recycling called Qwest to tell them that he sold them copper wire that appeared new and still had Qwest tags. A Qwest representative verified the copper wire as from the Prescott yard and said it

was not targeted for recycling. When detectives found the suspect, he allegedly told them he had worked in the telecommunications repair field for 10 years and knew the lingo so he was able to convince Qwest he was authorized to take the copper wire. He also told detectives he stole copper wire from the Qwest yard when no employees were around. Source: http://www.dcourier.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=87847

Nokia N8 smartphone struck by terminal power malfunction. Nokia's flagship N8 smartphone has been struck by a mysterious malfunction that causes it to abruptly power down permanently. According to Nokia, the problem points to an installation conflict connected to the handset's power management system and its internal engine. "We have dressed it down to the way we assemble the engines," commented the executive vice president in an AFP report, adding that "precautionary measures" have already been deployed in order to fully isolate the issue. However, although admitting there is an issue, a spokesman for the Finland-based company has been quick to note that the power outage has only affected an extremely small number of N8 devices. He also said the problem is covered by the handset's existing warranty and any device that cannot be properly repaired will be replaced with a new unit at no extra charge. Source: http://www.thetechherald.com/article.php/201046/6439/Nokia-N8-smartphone-struck-by-terminal-power-malfunction

Critical Manufacturing

Regulators move to combat potential engine-oil fires. U.S. and European regulators issued separate air-safety directives aimed at preventing oil leaks, fires and potentially hazardous engine failures on hundreds of airliners, including wide-body Boeing Co. jets and Airbus A380 super jumbos. The directives, issued November 22 by the Federal Aviation Administration (FAA) and the European Aviation Safety Agency, cover at least several dozen A380 engines made by Rolls-Royce PLC and roughly 900 other engines made by United Technologies Corp.'s Pratt & Whitney unit. The Pratt & Whitney engines are used to power some Airbus A300 and A330 models as well as such Boeing aircraft as the widely used 777 and 767 jets, according to the FAA. Airbus is a unit of European Aeronautic Defence & Space Co. The mandates highlight increased concerns by regulators and air-safety experts about the hazards of undetected oil leaks in jet engines. Such problems are believed to have prompted the blowout of a Rolls-Royce Trent 900 engine on a Qantas Airways Ltd. superjumbo A380 earlier this month, sparking an international investigation and prompting Qantas to ground its fleet of the aircraft. Source: http://online.wsj.com/article/SB10001424052748704243904575630930383298638.html

Toyota safety crash in spotlight after fatal Utah crash. The deadly crash of a Toyota Camry in western Utah is being blamed on a sticky gas pedal, the same problem that led the world's largest automaker to recall the car for repairs early this year. The 2008 Camry slammed into a rock wall near the Nevada border November 5, killing the driver and a passenger. The vehicle was the subject of three recalls, most recently for an accelerator that can get stuck in the open position. The crash raised questions about Toyota Motor Corp.'s system for repairing flaws in its vehicles. Safety advocates note that the government has received dozens of customer complaints about problems continuing even after a repair. A Toyota spokesman said the automaker was assisting the Utah Highway Patrol with its investigation. The automaker said it was too early to draw any conclusions about the cause of the crash. "We can't say definitely, but there is a strong likelihood that that in fact

did cause the crash," a police officer at the scene told the newspaper. Source: http://www.longislandpress.com/2010/11/18/toyota-safety-in-spotlight-after-fatal-utah-crash/

Defense/ Industry Base Sector

Schwartz concerned about F-35A delays. The Air Force Chief of Staff is concerned that delays in software engineering for the F-35A Lightning II Joint Strike Fighter could delay the service's fielding of the jet. He said that while the plane is ahead of schedule in terms of test flights, test points, and has had no "failures or surprises" structurally, delays in writing code for the plane have him worrying about whether it will reach initial operational capability by early 2016. "There are some issues with respect to timing on software development, and we don't have complete understanding on whether or not that will affect the IOC [initial operational capability] which was predicted after the Nunn-McCurdy assessment to be April of 2016," he said. The Air Force plans to buy 1,763 of the jets, making it the largest F-35 customer in the world. Source: http://www.dodbuzz.com/2010/11/23/schwartz-concerned-about-f-35a-delays/

Emergency Services

Future 911 system 'may accept text and video messages'. The U.S. Federal Communication Commission (FCC) is considering updating the 911 emergency call system to accept photo, text, and video messages. Roughly 70 percent of 911 calls are already being made from mobile telephones, said the FCC chairman. But the 911 system does not currently —support the communication tools of tomorrow, he added. The FCC said the Virginia Tech massacre was an incident when 911 multimedia technology could have been employed. —Some students and witnesses tried to text 911 during that emergency and as we know, those messages never went through and were never received by local 911 dispatchers, he said. But those multimedia messages may soon be answered due to broadband-enabled Next Generation 911, he said, in a speech at the Arlington County Emergency Center in Virginia. A system that would allow individuals to report crimes without being heard could also be used in situations ranging from kidnappings to robberies. The FCC Chairman added that texting is also a particularly useful form of communication for individuals who are deaf and others with a range of disabilities. Source: http://www.bbc.co.uk/news/world-us-canada-11824906

(Texas) **Copper thieves target radio transmission towers, endanger public.** A rash of break-ins at radio transmission towers in northern Harris and southern Montgomery counties in Texas have first responders worried about the impact on public safety. Thieves have broken into and stolen copper wiring from dozens of towers and, in at least one instance, disrupted the communications system dispatchers use to communicate with firefighters and paramedics. He said thieves broke into the fire department's transmission tower near Spring the week of November 15. They pointed the surveillance camera toward the sky and ripped apart a generator, he said. He said more than a quarter million people were put in danger because a communications outage triggered by the theft left dispatchers without a primary way to reach firefighters and paramedics for nearly 1 hour. According to sources inside various fire departments, thieves have targeted dozens of transmission towers in northern Harris and southern Montgomery counties for months. Thieves have also stolen copper pipes and copper wiring from a fire station under construction in Spring. Source: http://www.khou.com/news/Copper-thieves-target-radio-transmission-towers-endanger-public-109971859.html

ENERGY

Nothing Significant to Report

FOOD AND AGRICULTURE

(Oregon) **Organic dark chocolate squares recalled.** Artisan Confections Co., an Ashland, Oregon, organic chocolate maker owned by The Hershey Co., announced a recall November 24 after Salmonella was found in its product. The recall involves 33 cases of small, 0.32 oz tasting squares of its 74 percent cacao Dagoba —New Moon Organic Chocolate because they may contain Salmonella. The chocolate was sold nationwide online and through natural/specialty food retail outlets after October 27, 2010. The affected products were sold from display boxes labeled with the code 37HLB11, UPC 10474-55509. Source: http://www.foodsafetynews.com/2010/11/salmonella-prompts-recall-of-organic-chocolate/

Whole Foods recalls Bravo Farms cheeses. Whole Foods Market announced November 24 that it has carried many of the products involved in the recall of Bravo Farms cheese. Earlier this week Bravo Farms recalled its entire inventory due to evidence of Listeria and E. coli contamination at their Traver, California, plant. Bravo's products at Whole Foods Market stores in Arizona, California, Nevada, Oregon, and Washington are part of the recall; all were cut and packaged in clear plastic wrap and sold with a —Distributed by Whole Foods Market sticker. The following products are included in the recall: Sage Cheddar, Silver Mountain Cheddar, Chipotle Cheddar, Premium Block Cheddar, Premium White Chunk Cheddar, Chipotle Chunk Cheddar, and White Black Wax Cheddar. The Centers for Disease Control and Prevention announced November 25 that the number of those confirmed ill with E. coli O157:H7 infections after eating Bravo Farms raw milk Gouda-style cheese has risen to 38. That cheese was served or sold at Costco warehouses in Arizona, New Mexico, Nevada, Colorado, and the San Diego area. Source: http://www.foodsafetynews.com/2010/11/whole-foods-recalls-bravo-farms-cheese/

(Connecticut; Massachusetts) **Listeria prompts appetizer recall.** The USDA's Food Safety and Inspection Service (FSIS) discovered Listeria contamination at New Haven's Calabro Cheese, causing the Connecticut company to recall 57 pounds of its meat and cheese roll called Rotolini. The specific product is: 8-ounce packages of "Calabro All Natural Rotolini Mozzarella & Prosciutto." The packages also bear a white sticker with the lot number "3190" and establishment number "34051M" inside the USDA mark of inspection. The product was produced November 15 and distributed to warehouse and retail outlets in Boston and Springfield in Massachusetts and Westport, Connecticut. USDA said none of the product was purchased for the National School Lunch Program. No illnesses have yet been associated with the contaminated cheese. Source: http://www.foodsafetynews.com/2010/11/meat-cheese-recall-falls-under-usda/

(Washington) **New cheese recall: Washington State company pulls Mexican-style cheese.** The Food and Drug Administration announced a new cheese recall November 22. Del Bueno, located in Grandview, Washington, is pulling four Mexican-style cheeses over fears they are contaminated with listeria. The recall covers all packages of its Queso Fresco Fresh Cheese, Queso Panela Fresh Cheese,

Requeson Mexican Style Ricotta Cheese, and Queso Enchilado Dry Cheese. Source: http://www.perishablenews.com/index.php?article=0011133

(Nebraska) **Cozad man charged with failing to do mad cow disease reports.** A two-count indictment against a Cozad, Nebraska, man alleging that he provided false information to the U.S. Department of Health and Human Services (HHS) is among 23 indictments charging 25 defendants announced November 17 by a U.S. attorney. The indictments were returned by a federal grand jury for the District Court of Nebraska. According to a press release from the U.S. attorney, it is alleged the man provided false information to HHS on or about September 10, 2009, as an employee of the Nebraska Department of Agriculture. The man's job duties required him to contact cattle producers, perform inspections of cattle operations, and collect samples of cattle feed for the purpose of detecting potential contaminants such as bovine spongiform encephalopathy (BSE), also known as mad cow disease. The indictment alleged he provided false BSE reports to the Food and Drug Administration by stating he had made contact with and interviewed cattle owners, inspected premises, and collected samples of cattle feed when, in fact, he had not done so. The maximum penalty for this count includes 5 years imprisonment, a $250,000 fine, 3 years of supervised release, and a $100 special assessment. Source: http://www.kearneyhub.com/news/local/article_bd160750-f31e-11df-8d34-001cc4c03286.html

(California) **Residue gets in human food from animal drug misuse.** Tissue samples of a cow sold by Pastime Lakes Dairy near Lakeview, California, for slaughter as food to American Beef Packers Inc. were tested by the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) and found to contain flunixin residue at higher than allowed tolerance levels. According to a November 8 warning letter sent to Pastime by the Food and Drug Administration (FDA), the USDA tests found 0.162 parts per million (PPM) of flunixin in the liver tissue. FDA's tolerance level for flunixin in the edible tissues of an animal is 0.125 PPM. "Our investigation also found that you hold animals under conditions that are so inadequate that medicated animals bearing potentially harmful drug residues are likely to enter the food supply," the warning letter said. In an inspection conducted last September, FDA found Pastime was not following label instructions for flunixin meglumine and tetracycline hydrochoride, an anti-infective agent. Source: http://www.foodsafetynews.com/2010/11/residue-gets-in-human-food-from-animal-drug-misuse/

(Hawaii) **Quarantine proposed to stop spread of coffee borer beetle.** A state agricultural advisory committee has recommended an emergency quarantine on the Island of Hawaii to prevent the spread of a beetle that could severely damage Hawaii's $27-million coffee-farming industry. The board of agriculture is scheduled to meet at 8 a.m. November 23 at the plant quarantine office, 1849 Auiki St., to consider the measure.The advisory committee on plants and animals November 17 recommended a quarantine for 1 year on all coffee plants and unroasted beans in areas of Kona and Kau, unless farmers follow various procedures to reduce the spread of the coffee berry borer. The committee did not specify methods that might be used to kill the beetle and its larvae. Various methods to eliminate the beetle, including moisture reduction and heat and chemical treatments, were discussed during the public meeting, with the final list to be determined later. A statewide survey found the coffee berry borer, Hypothenemus hampei, present at 21 sites in Kona and Kau as of November 15. No other island was found to have the pest. Farmers in those areas will be required to have their products undergo a method of eliminating the beetles before coffee plants, parts of plants, unroasted beans, or related equipment can be transported elsewhere. Source:

http://www.staradvertiser.com/news/20101118_Quarantine_proposed_to_stop_spread_of_coffee_borer_beetle.html

Government Sector (including Schools and Universities)

Obama administration warns Congress pending WikiLeaks release will damage foreign relations. The U.S. President's administration said November 24 it has alerted Congress and begun notifying foreign governments that the WikiLeaks website is preparing to release sensitive U.S. diplomatic files that could damage U.S. relations with friends and allies. Officials said the documents may contain everything from accounts of compromising conversations with political dissidents and friendly politicians to disclosures of activities that could result in the expulsion of U.S. diplomats from foreign postings. U.S. diplomatic outposts around the world have begun notifying other governments that WikiLeaks may release these documents in the next few days. The release is expected the weekend of November 26, although WikiLeaks has not been specific about the timing. Source: http://www.chicagotribune.com/news/politics/sns-ap-us-wikileaks,0,232568.story

(California) **SDSU transit center shut down while police investigate suspicious package.** San Diego State University (SDSU) students, faculty, and staff were blocked from areas around the trolley station for almost three hours while the SDSU Police Department investigated an undisclosed, suspicious package which was later deemed nonthreatening. At approximately 1:40 p.m. November 23 an emergency alert was made on campus loudspeakers advising people to avoid the Transit Center, Aztec Center, and the Adams Humanities building. Those areas had been evacuated prior to the announcement. Security personnel and caution tape surrounding the entire area blocked people from passing through. When students approached the security, they were told that the area would be closed until further notice because of a potential bomb threat. SDSU police say the suspicious package was found by one of the trolley security members. "There was a piece of luggage located on the mezzanine level of the trolley station at SDSU," an SDSU police captain said. "After the San Diego Fire Department Metro Arson Strike Team evaluated it, it was determined to be non-explosive and safe to transport, although there was a chemical detected. Further initial investigation revealed it to be a substance similar to modeling clay and epoxyâ_¦It was rendered safe and the trolley station has since been reopened." Source: http://eastcountymagazine.org/node/4857

(Florida) **Fla. woman accused in school threats arrested.** A woman charged with making threats that caused 300 Florida schools to be locked down and a congressman-elect's top aide to step down was arrested November 23, federal authorities said. FBI agents apprehended the 48-year-old suspect of New Port Richey, Florida, near Los Angeles, the U.S. Attorney's Office in Miami said. She is accused of sending an e-mail on November 10 to a WFTL 850 AM conservative talk show host, who was tapped to be a U.S. Representative-elect's chief of staff. The suspect called the Pompano Beach station later that morning and claimed that her husband was going to go to a school in Pembroke Pines and start shooting, according to federal authorities who said they traced the call. Authorities responded by placing all 300 Broward County schools in lockdown for several hours. The talk show host has been on South Florida radio for nearly 20 years. She stepped down as chief of staff a day after the lockdown, saying she wanted to avoid any repercussions against the U.S. Representative. Source: http://www.bloomberg.com/news/2010-11-24/fla-woman-accused-in-school-threats-arrested.html

Security at U.S. courthouses questioned. Federal judges and court personnel could be at risk because of poor training, questionable contracts, and broken security equipment used by guards protecting the nation's federal courthouses, according to a new report by the Justice Department's inspector general. Federal courthouse security is handled by the U.S. Marshals Service, which employs about 5,000 contract guards to protect more than 2,000 federal judges and 6,000 other court personnel working at 400 facilities nationwide. But multiple district offices failed to detect mock explosive devices sent to them by agency officials in February 2009 as part of a test of local security procedures, the report said. Three unnamed federal district court chief judges at unspecified locations expressed serious concerns with security procedures, especially with how guards screen visitors and large vehicles entering courthouses. Names and locations were not published for security purposes, according to the inspector general's office. Federal court personnel were the target of 1,278 threats in fiscal 2008, more than double the threats received in 2003, according to an inspector general report published in 2009. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/22/AR2010112207052.html

(Florida) **Bomb threat forces St. Marys City Hall evacuation.** The Saint Marys, Georgia City Hall was evacuated for about 1 hour November 19 after a man told a police officer he planted a bomb in the building. No bomb was found. The threat also forced the evacuation of several businesses, including a day-care center, after police and fire officials established a 500-foot perimeter. St. Marys Elementary School was also locked down after the threat. A businessman and owner of James Jewelers was arrested for making a false public alarm, the police said. He was in city court waiting to appear before a judge on unspecified charges when the threat was made. An officer noticed the man leaving his seat several times, supposedly to go to the bathroom. The officer told him to stop leaving the courtroom when the man made the threat. After the evacuation, the bomb squad from Kings Bay Naval Submarine Base was called. A dog trained to sniff for explosives checked the building and a package was found, but it did not contain any hazardous devices. Source: http://jacksonville.com/news/georgia/2010-11-20/story/bomb-threat-forces-st-marys-city-hall-evacuation

(Iowa) **Dubuque City Hall evacuated for bomb threat.** One man's bomb threat closed down the entire city hall in Dubuque, Iowa, and blocked traffic for almost 4 hours November 18. A bomb squad discovered there was not anything explosive inside a suitcase left in front of city hall. A 68-year-old male now faces a charge of felony false report. Police said he claimed he had a bomb inside a suitcase. That caused police to shut down four blocks around the downtown Dubuque building, and evacuate several surrounding businesses. Two teenagers told police they saw the suspect carrying two black suitcases in front of city hall. He then made mention of some sort of an explosive device inside the bags. Police started blocking off the streets surrounding city hall around 3:30. Officers evacuated everyone working inside city hall, and the neighboring businesses. Source: http://www.kcrg.com/news/local/Dubuque--109032374.html

(Texas) **Area school threat may have originated in Saudi Arabia.** Authorities in Williamson County, Texas, and agents of the FBI believe an Internet-linked bomb threat against a school in Round Rock may have originated with a juvenile in Saudi Arabia. The Facebook-related incident led to the evacuation November 16 of two schools in the Round Rock Independent School District. After inspection authorities did not find any suspicious devices at either Deerpark Middle School or Live Oak Elementary School. A Williamson County sheriff's official said November 18 the suspect, who

could face charges, was never in Texas, and that the Deerpark school evidently was randomly targeted. The official said the suspect posed as a Deerpark student and also allegedly called several students. The FBI is also investigating. Making a false alarm or report is a state jail felony. Source: http://www.kwtx.com/home/headlines/109186454.html

(District of Columbia) **Commerce Department hit by series of power outages.** The work is getting done, but the lights keep going out at the Commerce Department's headquarters in downtown Washington D.C. — the latest of several problems at some of the region's federal buildings. Rooms in two sections of the massive Herbert C. Hoover Building on Constitution Avenue NW went dark November 17 for the fourth time in days. An outage last week forced an early dismissal for some workers, according to the department. The outages are also affecting a computer network linked to other parts of the building. Power was quickly restored November 17, and the outages have affected only 250 of the building's 3,000 workers, according to a department spokeswoman. Officials continue to inform workers about the outages and are asking the General Services Administration — which owns and operates most federal buildings — to address the problem. Antiquated electrical equipment is to blame, said a GSA spokeswoman. "We believe we have prevented some future problems by separating our construction-zone power load entirely from the problematic breakers, and we will continue to reduce the load on those breakers that have failed." Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/18/AR2010111806347.html

Information Technology and Telecommunications

34% of all malware ever created appeared in 2010. According to PandaLabs, in the first ten months of the year the number of threats created and distributed account for one third of all viruses that exist. These means that 34 percent of all malware ever created has appeared in the last 10 months. The company's database, which automatically detects, analyzes and classifies 99.4 percent of the threats received, now has 134 million separate files, 60 million of which are malware (viruses, worms, Trojans and other threats). In the year up to October, some 20 million new strains of malware have been created (including new threats and variants of existing families), the same amount as in the whole of 2009. The average number of new threats created every day has risen from 55,000 to 63,000. This would all suggest that the cyber-crime market is currently in rude health, although this is also possibly conditioned by the increasing number of cyber-crooks with limited technical knowledge who are turning their hand to these activities. This also means that although more malicious software is created, its lifespan is shorter: 54 percent of malware samples are active for just 24 hours, as opposed to the lifespan of several months enjoyed by the threats of previous years. They now infect just a few systems and then disappear. Source: http://www.net-security.org/malware_news.php?id=1545

ZeuS variant only infects super-fast PCs. Miscreants behind one variant of the ZeuS Trojan have outfoxed themselves in their attempts to outwit anti-virus analysts by releasing a variant of the malware that only infects high-performance PCs. Security firms use automation and virtualization technologies to cope with the growing volume of malware spewed out by cybercrooks every day. VXers are well aware of this and use virtual machine detection and anti-debugging code in their creations. The tactic is designed to frustrate security researchers and in so doing increase the time it takes to detect, develop, and distribute anti-virus updates. Users of the ZeuS crimeware toolkit are very much involved in this cat and mouse game between security researchers and cybercriminals. But

one particular group using the crimeware toolkit released a variant whose anti-debugging efforts are so aggressive it effectively assumes any machine whose CPU is running at lower than 2GHz must be running a debugger. As a result the malware only runs its malicious routines on high-performance machines, remaining inert on lower horsepower boxes. A security analyst at F-secure explains: —With a CPU below 2GHz the sample acts as if it is being debugged, aborts execution and does not infect the system. I tested the sample on an IBM T42 (1.86 GHz) notebook and the system was slow enough to avoid being infected. Source:
http://www.theregister.co.uk/2010/11/25/snobby_zeus_variant_avoids_bog_standard_pcs/

Kids lured to scam site by promises of parental control bypassing. The latest scam to hit Facebook users is one that supposedly offers a completely free proxy service for those who want to bypass parental controls and blocks set up by schools and at workplaces that prevent users from accessing certain sites such as Facebook. The campaign is specifically targeting kids, luring them into trying out the service located at hxxp://myfatherisonline.com to access Facebook in school. Sunbelt researchers have have poked around the site and discovered a veritable trove of various scamming attempts. The victims are faced with an affiliate site containing malware, surveys, quizzes, and offers for free iPhones that will try to get them to subscribe to a premium rate service or sign up for spam. Source:
http://www.net-security.org/malware_news.php?id=1546

Facebook news feeds beset with malware. One fifth of Facebook users are exposed to malware contained in their news feeds, claim security researchers. Security firm BitDefender said it had detected infections contained in the news feeds of around 20 percent of Facebook users. Facebook said it already had steps in place to identify and remove malware-containing links. BitDefender arrived at its figures by analyzing data from 14,000 Facebook users that had installed a security app, called safego, it makes for the social network site. In the month since safego launched, it has analyzed 17 million Facebook posts, said BitDefender. The majority of infections were associated with apps written by independent developers, which promised enticements and rewards to trick users into installing the malware. These apps would then either install malware used for spying on users or to send messages containing adverts to the users' contacts. Facebook said it had processes and checks in place to guard against the risk of malware. "Once we detect a phony message, we delete all instances of that message across the site," the site said in a statement. Source:
http://www.bbc.co.uk/news/technology-11827856

Multiply users urged to download disguised malware. Users of the Multiply social networking site have lately been targeted with malicious personal messages coming from accounts opened by cybercriminals. The message implies that the sender and the recipient know each other from somewhere, and the potential victim is urged to see the attached movie in order to jog their memory. But, the movie is just a pretext to get him or her to install a codec that is supposedly needed to see the video. The offered codec is a dropper Trojan in disguise. It is detected by Trend Micro as TROJ_KATUSHA.F, and it is also often sent out as an attachment in bogus e-mails. Source:
http://www.net-security.org/malware_news.php?id=1542

Are malware hybrids the next big threat? Recent encounters with hybridized malware files have left Trend Micro researchers wondering if they have been designed that way or if they are just an undesirable side effect lurking from heavily infected systems. To demonstrate how both malware may benefit from the symbiosis, they took the recently detected attack involving an IRC bot

(WORM_LAMIN.AC) infected by a mother file infector (PE_VIRUX.AA-O) as an example. Because of PE_VIRUX's polymorphic nature, WORM_LAMIN.AC might be harder to detect. WORM_LAMIN.AC returns the favor by spreading PE_VIRUX. Together they change user and system security settings in a way that makes it easier for them to remain undetected, and payloads carried by both are delivered. It is likely that its appearance will spark other malware developers to try that novel approach. Source: http://www.net-security.org/malware_news.php?id=1540

iOS 4.2 includes massive security update. Apple has released iOS 4.2. The update fixes more than 80 vulnerabilities in the iPhone, iPod, and iPad. Apple policy dictates that the vulnerabilities not be publicly disclosed until the patch is available. Many of the vulnerabilities had critical security implications. For example, viewing a PDF file was a potentially risky task on pre-iOS 4.2 devices. —A heap buffer overflow exists in FreeType's handling of TrueType opcodes [CVE-2010-3814]. Viewing a PDF document with maliciously crafted embedded fonts may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue through improved bounds checking, Apple said. There is also a vulnerability which reveals surfing history. —A design issue exists in WebKit's handling of the CSS :visited pseudo-class. A maliciously crafted website may be able to determine which sites a user has visited. This update limits the ability of web pages to style pages based on whether links are visited. Source: http://www.computerworld.com/s/article/9197839/iOS_4.2_includes_massive_security_update

Spam hole in Google Mail. Until recently, a security hole in a Google API allowed e-mails to be sent to GMail users without knowing e-mail addresses. As reported by TechCrunch, victims only had to visit a specially crafted Web site while being logged into their Google account. Apparently, the hole could even be exploited while in Private Browsing mode, which does not usually give access to a user's cookies. The vulnerability allowed e-mails with arbitrary subject lines and message bodies to be sent from the e-mail address noreply@google.com. As the e-mails included an authentic header, it was virtually impossible for users to distinguish them from an authentic e-mail sent by Google. The hole was discovered by a 21-year-old Armenian, who made his demo exploit freely accessible on Google's Blogspot / Blogger service. Google shut the blog down shortly after the exploit was reported, and confirmed the problem in an e-mail to TechCrunch. Google said the hole in its Apps Script API has now been traced and fixed. Source: http://www.h-online.com/security/news/item/Spam-hole-in-Google-Mail-1139762.html

Kroxxu botnet hits a million web users. Security experts have uncovered a dangerous new botnet which has already infected over 100,000 domains and 1 million systems worldwide, although it is still unclear how the cyber criminals are monetizing their efforts. The Kroxxu botnet has been designed solely to steal FTP passwords but, unlike traditional botnets, it is able to spread through infected Web sites alone rather than individual PCs, according to researchers at Avast Software who have been tracking it for over a year. The stolen passwords enable Kroxxu's creators to add a script tag to the original Web site content, which then makes it possible to upload and modify files on infected servers and spread to other servers globally. The malware relies heavily on redirects to obfuscate itself, while various components of the network are able to perform different roles, known as " indirect cross infection". "Kroxxu's indirect cross infections are based on all parts being equal and interchangeable," said the head virus researcher at Avast. Avast has not yet discovered how the botnet organizers are making money from the scam, but the researcher suspects they could be selling stolen credentials or hacked space on infected servers, or using key-loggers to spread other spam. The botnet has infected

1,000 domains a month since its discovery in October 2009, and many of the PHP redirectors and malware distributors placed in the sites have survived for months at a time. By infecting legitimate sites, the botnet could have a serious impact on the success of URL blocking software, warned Avast. Source: http://www.v3.co.uk/v3/news/2273368/kroxxu-avast-botnet-threats

McAfee warns users against 12 online scams this Christmas. McAfee has revealed the 12 most dangerous online scams computer users should be cautious in this holiday season. The "Twelve Scams of Christmas" include iPad offer scams, "Help! I've Been Robbed" scam, fake gift cards, holiday job offers, "Smishing", suspicious holiday rentals, recession scams, Grinch-like greetings, low price traps, charity scams, dangerous holiday downloads, and hotel and airport wi-fi. McAfee Labs director of security research said scams continue to be big business for cybercriminals who have their sights set on capitalizing on open hearts and wallets. McAfee advised Internet users to follow five tips to protect their computers and personal information in lieu of these cyber threats. The security firm has advised users to stick to well-established and trusted sites, and not to respond to offers that arrive in a spam e-mail, text, or instant message. McAfee also advised online users to preview a link's Web address before clicking, to stay away from vendors that offer prices well below the norm, and to only use trusted wi-fi networks. Source: http://security.cbronline.com/news/mcafee-warns-users-against-12-online-scams-this-christmas_161110

Apple patches critical 'drive-by' Safari bugs. Apple November 18 patched 27 vulnerabilities in Safari for Mac OS X and Windows, 85 percent of them critical bugs that could be exploited to hijack Macs or PCs. Of the 27 flaws fixed in Safari 5.0.3 for Mac and Windows, four were patched by Apple in September in its iOS mobile operating system, and at least three had been addressed by Google in its Chrome browser as far back as mid-August. Chrome and Safari share the open-source WebKit browser engine. Apple identified all 27 vulnerabilities it patched as within WebKit. Most of the vulnerabilities addressed in the Safari updates — Apple also patched the older Safari 4 that runs in Mac OS X 10.4, aka Tiger — were accompanied by the phrase "arbitrary code execution," which is Apple's way of saying "critical." According to Apple, the 23 critical bugs can be exploited by "drive-by" attacks that launch as soon as a victim browses to a malicious Web site. Among the non-critical vulnerabilities was one that could be used by unscrupulous site owners to secretly track users' browsing habits, even when Safari has disabled cookies. Another flaw could let identity thieves spoof the URL showing in Safari's address bar, a common tactic of phishers who feed bogus sites to users in the hope of capturing passwords to online bank accounts. Source: http://www.computerworld.com/s/article/9197184/Apple_patches_critical_drive_by_Safari_bugs

German hacks national security agency's hashing algorithm. A German hacker has claimed to have hacked the national security agency's Secure Hashing Algorithm (SHA1) using rented computing resources. The hacker used GPU-powered rented computing resources to crack 10 out of the 14 SHA1 passwords he was aiming for. He used brute force attacks to achieve the hack in 49 minutes. He managed to hire the computing resources used to hack the SHA1 encryption for $2. Security experts have warned for quite some time that the once powerful password encryption technique is no longer safe to use. Source: http://www.itproportal.com/2010/11/19/german-hacks-national-security-agencys-sha1/

National Monuments and Icons

(California) **Snow strands travelers in national forest.** Two cases of stranded travelers in Mendocino National Forest in California were reported November 21. Just after noon, three people were reported to be suffering from exposure to the new-fallen snow in the forest area above Upper Lake, according to radio reports. Two people of Northshore Fire Protection District tried to make their way up to assist. —We could not reach them, one said November 22, noting, —We got as far as we could. But U.S. Forest Service personnel were able to assist the three individuals. On the Mendocino County side of the forest, 12 people had to be rescued after becoming stuck in the snow, according to a captain of the Mendocino County Sheriff's Office. Shortly before 7 p.m., the Mendocino County Sheriff's Office was advised that 12 people had traveled from the Willits and North County area to the Anthony Peak Range. Once in the Anthony Peak Range area, the dozen individuals became stuck in the snow and called for help from their cell phones. Mendocino County Search and Rescue were dispatched to the location. At 11 p.m., four of the stranded subjects were able to walk to the location where a search and rescue group was staged, but the weather and road conditions were such that the remaining eight could not be reached safely until it was daylight and there was a break in the weather. The stranded subjects were advised to stay inside of their vehicle until help reached their location. At 7:30 a.m. November 22, deputies utilized Mendocino County Sheriff's Office snowmobiles and were able to access the remaining eight individuals who had remained at their vehicles. Source: http://lakeconews.com/content/view/17106/919/

(Utah) **Suspect in Utah park ranger's shooting is at large.** Scores of law enforcement officers are scouring rugged terrain in Utah for a wounded man they said repeatedly shot a park ranger, authorities said. "He is wounded, and on foot," said the Grand County, Utah, sheriff, who is leading the search. The ranger was shot multiple times November 19 while on patrol on the Poison Spider Mesa Trail area near the city of Moab, according to the Grand County Sheriff's Department. Marked by cliffs, dry canyons and rocky terrain, the trail is a haven for mountain bikers as well as hikers. The ranger had stopped the man in his vehicle, then was shot in the arm, leg, and stomach as the two exchanged gunfire, according to KSL. The 34-year-old victim was airlifted to a hospital, where he was conscious and talking to officers, KSL said. Local, state, and federal authorities have since teamed up to look for the suspect. They include 130 officers from the sheriff's department, Utah state agencies, the FBI, the National Park Service, and local police departments. Source: http://edition.cnn.com/2010/CRIME/11/20/utah.ranger.shot/

(Ohio) **Stretch of Ohio forest closed during coal fire.** A 5-acre area of Ohio's only national forest will remain closed while authorities try to put out an underground coal fire. The Columbus Dispatch reported forest managers plan to hire a contractor to locate the source of the fire and then suppress it using a mix of water and soil. Federal firefighters located the fire after spotting small amounts of smoke coming up during a routine patrol in Wayne National Forest near Nelsonville in southeast Ohio. An emergency order November 19 closed the area while heavy equipment is brought in to help extinguish the fire. Forest officials warn there could be fumes and unstable ground in the area. They said the fire is near where an April brush fire spread over some 100 acres. Source: http://www.daytondailynews.com/news/ohio-news/stretch-of-ohio-forest-closed-during-coal-fire-1008296.html

Postal and Shipping

Fedex package with radioactive material missing. A package containing radioactive material has disappeared in transit. The package, containing material known as —GE 68 was shipped, by FedEx, from Fargo, North Dakota to Knoxville, Tennessee. But when it was opened the GE 68 was missing. A spokesperson from Federal Express told WGN that there should not be any threat to public safety, as long as the package is not tampered with. The Nuclear Regulatory Commission (NRC) has notified public safety agencies. Among those agencies notified of the incident by the NRC include the CDC, the FBI, the EPA, and the Department of Homeland Security. Source: http://www.wgntv.com/news/wgntv-fedex-radioactive-package-nov25,0,3949749.story

Postal service IG examines cyber incident data. The inspector general of the U.S. Postal Service (USPS) is auditing a database that tracks USPS cyber incidents to determine whether the information it has been collecting is reliable, said agency officials in the Office of the Inspector General (IG). The review, which the IG's office launched on November 22, comes at a time when officials are increasingly concerned about a new computer worm, Stuxnet, that has the power to cripple industrial operations on a global scale. For the Postal Service, which has a role in virtually every citizen's life, a systemwide outage could undermine the economic viability of the country, as well as public confidence, security experts said. Its reliance on highly automated distribution and scheduling systems for air mail, truck delivery and rail transport make cybersecurity a critical issue for the agency, a vice president at a national security consulting firm said. IG officials said they decided to audit USPS incident data in the wake of the White House's call for all agencies and the public to better defend against the growing cyber threat to national security. Cybersecurity is a top priority for the current Presidential administration, said a USOIG spokeswoman, adding audits can last anywhere from three to six months. Source: http://www.nextgov.com/nextgov/ng_20101124_2562.php

(Oregon) **Arrest in bomb threat case brings federal charges.** A 61-year-old Corvallis man arrested by Eugene Police officers on November 24 now faces a federal charge of using a telephone to threaten to bomb a federal facility. The FBI and the U.S. Postal Inspection Service jointly investigated this alleged threat against the post office in Eugene, Oregon. The suspect is currently lodged at the Lane County Jail. He will make his initial appearance before a federal judge at 1:30 p.m. on November 18th, at the U.S. District Courthouse in Eugene. The Assistant United States Attorney is prosecuting this case. Source: http://www.ttkn.com/law-and-order/arrest-in-bomb-threat-case-brings-federal-charges-6105.html

(New York) **Parcel alarms post office.** A package leaking an unidentified substance at the post office caused emergency responders to shut down a portion of St. Regis Road in Hogansburg, New York November 19. A U.S. Postal Service inspector said the package —arose some suspicions with the employees. St. Regis Mohawk Tribal Police said about 4 ounces of a substance spilled from the package. Officials would not identify the substance. While the typical protocol would have required the employees to notify the U.S. Postal Service, the Postal Inspector said the local employees instead contacted Franklin County 911, which dispatched its hazardous materials unit. She said postal inspectors also responded to the scene once notified of the incident. Source: http://www.watertowndailytimes.com/article/20101123/NEWS05/311239960

PUBLIC HEALTH

(Massachusetts) **New sensor could detect quickly viral bioterror agents.** Scientists at Boston University have developed a biological sensor that could be used to rapidly detect a wide range of viral pathogens including the lethal Ebola and Marburg viruses, the institution announced November 17. As with other viruses that produce symptoms not necessarily indicative of viral infection, Marburg and Ebola outbreaks can be challenging to diagnose. The situation could be further complicated by the current reliance on diagnostic systems that need substantial supporting infrastructure and require a lengthy period for biological sample preparation. The developmental biodetector, however, is capable of sensing active viruses with —little to no sample preparation, according to a Boston University press release. —Our platform can be easily adapted for point-of-care diagnostics to detect a broad range of viral pathogens in resource-limited clinical settings at the far corners of the world, in defense and homeland security applications as well as in civilian settings such as airports, the research team leader said in released comments. —By enabling ultraportable and fast detection, our technology can directly impact the course of our reaction against bioterrorism threats and dramatically improve our capability to confine viral outbreaks. The scientists received university funding as well as financing from the U.S. Army Research Laboratory. Through joint research with the U.S. Army Medical Research Institute of Infectious Diseases, they were able to prove the biodetector's capability to sense in a typical laboratory environment the presence of hemorrhagic fever virus surrogates and pox viruses such as smallpox or monkeypox. —The new biosensor is the first to detect intact viruses by exploiting plasmonic nanohole arrays (PNAs), or arrays of apertures with diameters of about 250 to 350 nanometers on metallic films, that transmit light more strongly at certain wavelengths, according to the press release. Source: http://gsn.nti.org/gsn/nw_20101124_7290.php

FDA releases drug shortage list. There are 150 prescription drugs on the Food and Drug Administration's (FDA) shortage list. The list includes many drugs that are used in hospitals — including painkillers such as morphine and many cancer treatment drugs. The FDA has a list of reasons for the drug shortages on its website. Source: http://www.clickondetroit.com/health/25896874/detail.html

(North Carolina) **NC man poses as doctor at hospital ER for weeks.** A North Carolina man faced criminal charges after police say he posed as a health professional and got involved with patients at a hospital emergency room. The 24-year-old man was charged with three misdemeanor counts of impersonating a doctor, multiple media organizations reported November 24. He posed as a visiting medical resident seeking training and camped out in the emergency room of Cape Fear Valley Medical Center. He said he was at it for two weeks in October before a physician assistant noticed he was not wearing a badge in the emergency department. The hospital said he was shadowing doctors and nurses and was never alone with a patient. The accused is "a troubled young man with a history of impersonation, or similar activity," a hospital spokesman said in a statement. The man said he has a medical degree from the University of Tennessee, but the school has no record of him being enrolled, the Fayetteville Observer reported. "My job is to observe and be a helping hand if needed and to further medical assessment," he told WTVD-TV. The hospital has launched an internal investigation to determine how many patients the man may have come in contact with. Source: http://www.heraldonline.com/2010/11/24/2639936/nc-man-poses-as-doctor-at-hospital.html

(Illinois) **Norovirus outbreak in three facilities; 129 people ill.** An outbreak of norovirus has been reported after 129 people became ill in three long-term care facilities, according to the McHenry County Department of Health (MCDH) in Illinois. Fourteen cases of norovirus, which is highly contagious, have been confirmed and five people have been hospitalized. An MCDH spokeswoman declined to release the names of the facilities where the virus was found, but said that their administrators are cooperating and taking steps to prevent it from spreading. Unlike influenza, which is an upper respiratory virus, noroviruses are generally the culprit that causes what is referred to as —stomach flu. It affects the intestinal tract and causes nausea, vomiting, and diarrhea. Symptoms usually last between 24 and 48 hours. Source: http://www.nwherald.com/2010/11/22/norovirus-outbreak-in-three-facilities-129-people-ill/ah5cxnj/

FDA pulls Darvon painkiller due to safety risks. The U.S. Food and Drug Administration (FDA) said November 19 that Xanodyne Pharmaceuticals had agreed to halt all U.S. marketing of Darvon and the related brand Darvocet, which have been subject to safety concerns for decades. The Kentucky company confirmed the move in its own statement. The FDA also ordered generic drugmakers to stop making and selling low-cost drugs containing the active ingredient in Darvon, called propoxyphene. FDA officials said they decided to take action based on a recent study showing Darvon interferes with the electrical activity of the heart, causing irregular heart rhythms that can be fatal. Xanodyne conducted the study last year at the government's request. Source: http://www.forbes.com/feeds/ap/2010/11/19/general-us-painkiller-withdrawal_8153251.html

TRANSPORTATION

(Florida) **Florida airport considers ditching TSA.** An Orlando, Florida, airport official wants to join the small group of U.S. airports who use a private company to screen passengers instead of the Transportation Security Administration (TSA). The airport first considered the change in February and it was approved October. 5. According to the president of the Sanford Airport Authority in Orlando, research shows that using a private security screening company would be "more efficient and more enjoyable to the public." His comments come during a week in which the TSA has been under fire for it's airport screening procedures, including imaging technology and pat downs. The TSA currently lists 16 airports that are participating in its Screening Partnership Program. Source: http://edition.cnn.com/2010/TRAVEL/11/19/private.airport.screening/

(Florida) **Miami International Airport 'skycaps' caught in baggage scam.** Dozens of curbside baggage handlers at Miami International Airport in Miami, Florida accepted cash payoffs from travelers to check in extra or overweight bags or boxes — creating a possible security risk and adding extra, unrecorded pounds to airliners, authorities said. Miami-Dade police arrested 15 baggage handlers November 17 employed by Eulen America, the company contracted to check in luggage for American Airlines. The sweep concluded a 9-month investigation spearheaded by Miami-Dade police airport district detectives, American Airlines security, and state prosecutors. Investigators believe the travelers were mostly business operators shipping goods to Latin America who had cultivated relationships with skycaps over months or years. The probe revealed the travelers would call and arrange the deals with skycaps days in advance. In some cases, unaccompanied bags were sent through — an apparent violation of federal transportation regulations for international flights. Source: http://www.miamiherald.com/2010/11/17/1931088/airport-skycaps-caught-in-baggage.html

(Colorado) **Patience wears thin as FAA equipment problem returns.** After a third unsuccessful start-up, a navigational aid atop Aspen Mountain in Aspen, Colorado used to guide planes landing at the airport shut off November 17, prompting a federal aviation director to meet with frustrated and uneasy local officials at city hall November 18. The Federal Aviation Administration has been working on replacing the equipment since October 8, when officials estimated it was a 2-week project. With problems persisting for more than 1 month since, and ski season less than 1 week away, several local officials foretold calamitous local economic repercussions if it isn't up and running soon. The inoperable system affects most flights into Aspen, which are operated by SkyWest for United Airlines. The airport's other carrier, Frontier Airlines, is unaffected because it uses global-positioning technology to land and does not need the on-the-ground aid. Source: http://www.aspendailynews.com/section/home/143775

Water and Dams

(Michigan) **10M gallons of sewage released into Saginaw River.** Facility officials say the Saginaw Water Treatment Plant has discharged 10 million gallons of untreated or partially treated sewage into the Saginaw River. Officials tell the Saginaw News the release happened between the night of November 22 and the morning of November 23 following a 1.75-inch rainfall that caused four retention basins to overflow. Water treatment officials at the mid-Michigan plant say they pretreated the sewage with hypochloride. They also allowed solids to settle before discharging overflow. Officials tested for E. coli at two points along the river. Results are pending. Source: http://www.chicagotribune.com/news/chi-ap-mi-sewagedischarge-s,0,6154850.story

(Utah) **Dangerous levels of mercury in Park City's water.** Park City, Utah, in conjunction with the Utah Division of Drinking Water, is running tests the week of November 15 after high levels of mercury and other metals were found in five areas. Complaints of off-color water came pouring in after the city changed drinking water sources to allow for snow making at Park City Mountain Resort, according to the city water manager. About 300 residences and businesses in Thaynes Canyon, Aspen Springs, Saddle View, Iron Canyon, and Park City Mountain Resort have been advised not to drink or cook with tap water. Last week, the municipality switched its Spiro Tunnel water to Park City Mountain Resort for the ski season. At the same time, it turned on its Judge Tunnel and Thiriot Springs sources to fill municipal drinking water needs. A decrease in water acidity, or pH-level, made the water more corrosive, the water manager said. The more acidic water could be dissolving buildup in pipes, she said. Mercury readings jumped from a permissible 2 parts per billion to as high as 16 parts per billion in affected areas. Arsenic, manganese and thallium were also identified at unacceptable levels, according to the director of the state division of drinking water. Officials believe the problem lies with the Thiriot Springs water. It will be diverted to the Spiro Water Treatment Plant where its pH can be adjusted. Ongoing tests should reveal whether the plan is working. Source: http://www.sltrib.com/sltrib/home/50696942-76/park-drinking-levels-mercury.html.csp

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**